



◆ 導入事例

株式会社日立システムアンドサービス

HitachiSystems

財務本部 財務部 部長代理  
戸松敏美 様 (左)  
プラットフォーム  
ソリューション本部  
加藤利昭 様 (右)



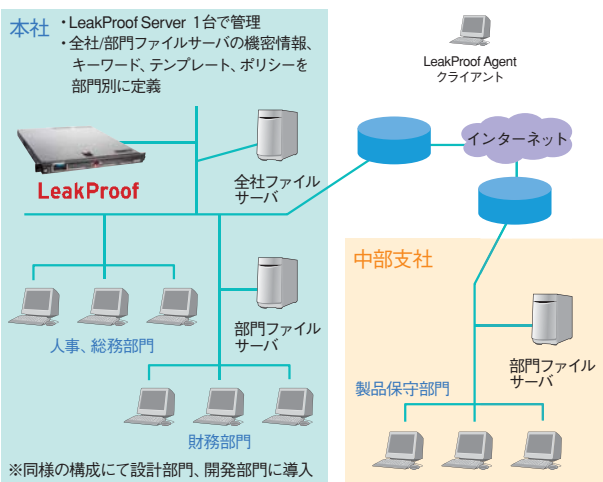
一般企業における情報漏えいの約8割は内部からの流出が原因と言われている。株式会社日立システムアンドサービスでは、本格的な情報漏えい対策に乗り出した。社内の顧客データや社員の人事データなどの個人情報のほか、開発部門の仕様書やソースコードなどの技術情報や財務の決算データなど、各種情報を扱うのが人間である限り、誤操作や誤送信により機密データを流出させてしまうようなミスは起こり得る。そこで同社は、情報漏えい対策としてTrend Micro LeakProofを導入した。結果として社員への負担は発生せず、より強固なセキュリティ環境を実現した。

誤操作、誤送信などのヒューマンエラーによる  
重要データ流出をクライアントレベルで防止。  
社員に負荷はなく、確実なセキュリティ環境を構築。

- ◆導入時期  
2007年10月
- ◆導入台数  
1台
- ◆ライセンス数  
100ユーザ



日立システムアンドサービスLeakProof導入イメージ図



■導入企業プロフィール

会社名：株式会社日立システムアンドサービス  
設立：1978年9月21日  
本社：〒108-8250 東京都港区港南2-18-1

代表：執行役社長 中村博行  
資本金：41億9千万円 (2007年3月31日現在)  
従業員数：4,817名 (2007年3月31日現在、連結)

事業：クライアントサーバシステム、ネットワークシステムの設計・開発・販売、インターネット・システム構築サービス、ホスティングサービス、ハウジングサービス、ASP など幅広く手掛ける。

URL : <http://www.hitachi-system.co.jp>

## 導入背景

「情報漏えいの約8割は内部からの流出という現実を受けて」

日立システムアンドサービス（以下、日立システム）は、SI、ソフトウェア開発、ハードウェア及びソフトウェア販売の分野で相互連携の強みを生かした事業を展開している。そのため、部門ごとに様々な情報を扱っている上、内容が大きく異なる。契約書・見積書はもちろん、開発に係わる仕様書や設計図などの技術情報、顧客データ、未公開の決算書類など機密情報も多い。同社は漏えい対策には万全の対策を取りたい考えだ。

以前から日立システムでは、執行役クラスをトップにした情報セキュリティ委員会を設けており、漏えい対策には万全の対策を取っている。こうした背景の中、プラットフォームソリューション本部の加藤利昭氏は不注意による漏えい防止をより強化するため、新たな対策製品を検討した。

「企業内部からの情報漏えいはいまだ後を絶ちません。ひとたびこうした事故が起きた時、企業の責任は重大です。そのため、どんなクライアントにも柔軟に対応できる情報漏えい対策が必要と考えていました」（加藤氏）

情報漏えい対策と一括りにしても、その対策方法は様々だ。しかし、情報漏えいを引き起こす原因の8割を占める人がミスに対してどこまで対策を行えば十分なのかという不安は残る。日立システムではこれまでに暗号化ソフトで重要なファイルの暗号化を行ったり、社内のPC使用にポリシーを定め、フリーソフトを原則使用禁止にしたり、持ち出し用のPCにはHDDレスのセキュリティPCを利用するなどの対策を施してきた。しかし加藤氏は「対策を重ねれば重ねるほど、業務フローに変更が生じ、業務効率の低下を引き起こす可能性が増幅するという懸念があるのも事実です」と語る。

そこで社内の各部門で行われている業務フローを変更することなく、全社員のPCからの情報漏えいリスクを回避することが今回の製品選定の重要課題となった。



株式会社日立システムアンドサービス  
プラットフォームソリューション本部

加藤利昭氏

## 選定ポイント

「LeakProofなら業務フローはこれまでとまったく変わりません」

加藤氏は重要データの扱いをクライアントレベルで制御できるTrend Micro LeakProof（以下、LeakProof）に着目した。

「重視したのは既存の業務フローを変更しないこととサポートがしっかりしていることです。というのも、社内にはIT部門のようなリテラシーの高い部署の人間だけではないことを考慮しなければならないからです」（加藤氏）

社内で真っ先に導入された財務本部 財務部の戸松敏美部長代理は「財務部の社員は財務処理が専門ですから更新作業やクライアントへの負荷を考えると、これまで通りのフローで業務を行いたいという思いがありました」と語る。

LeakProofではクライアント側で行う作業や業務フローを変えることなく、情報漏えい対策を実現する。

まず、社内の重要データに対していわば指紋となるフィンガープリントを“DataDNA”と呼ばれるオリジナルの技術を用いて作成する。そしてフィンガープリントの情報はウイルス定義ファイルのように社内のクライアントPCに配信され、フィンガープリントの情報を元にクライアントPCは、ファイルが「社外秘であるか」、「社員がどう扱うか」を判断し、メールやweb、USBメモリ経由などからの情報流出をブロックするのである。この方法はファイル名の変更や内容の一部をコピーして社外へ持ち出そうとした場合でも、フィンガープリントの一部から元ファイルを判断し、流出をブロックする。誤って重要なファイルをメール送信しようとした場合も同様だ。

「社内の（部門的）に何が重要なデータかを定義ファイルとして配信してくれるので重要なデータかどうかを社員自身が判断しなくても良いため効率的です。財務データを管理するクライアントPCに導入していますが、導入後も社員から不満の声



株式会社日立システムアンドサービス  
財務本部  
財務部  
部長代理

戸松敏美氏

はありません。情報漏えい対策の導入に際しての“業務フローを変えない”という目的が達成できました」（戸松氏）。

## 導入効果

「メリットはケアレスミスを防ぐことだけではありません」

LeakProof導入には重要データの定義が必要となり、日立システムでは綿密なヒアリングを行った。重要なデータの種類も定義も各部署で大きく違う。それらを各部署の上長らとLeakProofの管理を担当する加藤氏らで洗い出し、LeakProofで保護すべき重要なデータを抽出していった。

「この作業を事前に行うことが重要で、運用時のトラブル減につながります。またポリシーを定めてデータを抽出していく中で、社内の重要なデータは何か、どんな知財があるのかといった情報資産を把握することもできました」（加藤氏）

こうして各部署から上がってきた重要データに、フィンガープリントを作成し、それを部内の各クライアントに配信した。クライアント側では、HTTP、メール、USBメモリなどで「外部に持ち出そうとする行為」をエージェントソフトがフィンガープリントを元にチェックしてブロックする。チェック内容はファイルごとに扱いを細かく設定できるため、社員の作業はこれまで通り行える。

「例えば、財務部では重要データとして公開前のIR用財務データを設定していますが、こうしたデータは決算発表後は重要レベルが下がるため、「公開日以降は指定から外す」という期間指定で運用しています。逆に未公開時でも税理士など必要な相手に対してはデータを送信できる設定にしています」（戸松氏）

フィンガープリントの「定義ファイル」のデータサイズは非常に小さく、LeakProofのエージェントソフトによってクライアントPCの動作が重くなることもまったくなく、財務部の業務に支障はなかった。それよりも、うっかりミスが防止できることで社員には安心感が広がっているという。

## 将来展望

「社内の全クライアントに導入し、社員の意識も高めたい」

現在では、機密情報と定義される重要情報を取り扱う端末のみ限定して対象となる部署へ、LeakProofを先行導入しているが、今後約4,800人いる社員全員のPCに適用するように準備を進めている。

また同時に社員へのセキュリティ教育も定期的に行っているという。

「以前から社員は定期的にセキュリティ教育を受けているが、実際に部内で重要データの定義が共有され、それがLeakProofで守られていることで社員のセキュリティ意識が高まる、といった副次的な効果もあったようです」（加藤氏）

情報漏えいは、企業の信頼を一気に失墜させてしまう危険性ははらんでいる。しかし、クライアントPCからの漏えいが危険だからといってメールやUSBメモリの利用を制限しては、せっかくのIT資産を有効活用できない。そのジレンマの解決策として、LeakProofは有効な回答の1つとなった。

## トレンドマイクロ BIZ FOCUS 機密情報の情報漏えい対策に特化した製品LeakProof

日立システムの事例にもあるとおり、LeakProofは誤操作などによる、企業内部から情報流出を食い止める専用システムだ。

新たに発表されたバージョン3.0では主な機能にUSBなどへの書き出し時に有効な暗号化機能がある。ファイル書き込み時に自動的にパスワードを設定し、持ち出された機密情報を紛失した際の情報漏えいのリスクを低減させる。また、持ち出し可能なクライアントPCに対して、LeakProofサーバとアクセスできない状況の規制ルールを設定できるほか、プリントスクリーン機能の使用を禁止できる機能などもある。これでPCの盗難や紛失といったトラブル時にも、PC内の情報にはアクセスできないため安心だ。

いま、個人情報保護法やいわゆる日本版SOX法など、企業に十分な対策が求められている。LeakProofなら社内からの情報漏えいを阻止する有効な手立てとなるだろう。

【お問い合わせ先】

トレンドマイクロ株式会社  
東京本社 〒151-0053 東京都渋谷区代々木2-1-1 新宿メインズタワー  
TEL: 03-5334-3601 (営業代表) FAX: 03-5334-3639

◆ 製品の詳細についてはこちらから  
トレンドマイクロの製品情報サイト: <http://jp.trendmicro.com>

安心を、ひとつ上のステージへ。



HSS-LP-J001